

Weighted Simple Games as Access Structures of Ideal Secret Sharing Schemes

Ali Hameed and Arkadii Slinko

Abstract

Beimel, Tassa and Weinreb (2008) and Farras and Padro (2010) partially characterized weighted simple games that are access structures of ideal secret sharing schemes; they did this in terms of the operation of composition of simple games. They classified such indecomposable weighted games, and proved that any other weighted game, which is the access structure of an ideal secret sharing scheme, is a composition of the indecomposable ones. It remained unclear which compositions of indecomposable weighted games of this sort are weighted. In this paper we fill the gap by obtaining an if and only if characterization of weighted simple games that are access structures of ideal secret sharing schemes.

1 Introduction

Secret sharing schemes are modifications of cooperative games to the situation when not money but information is shared. Instead of dividing a certain sum of money between participants, a secret sharing scheme divides a secret into information shares—which are then distributed among participants—so that some coalitions of participants have enough information to recover the secret (authorised coalitions) and some (nonauthorised coalitions) do not. A scheme is perfect if it gives no information about the secret to nonauthorised coalitions. A perfect scheme is most informationally efficient if the shares contain the same number of bits as the secret [12]; such schemes are called ideal [20]. The set of authorised coalitions is said to be the *access structure*.

However, not every access structure can carry an ideal secret sharing scheme [20]. Finding a description of those which can carry appeared to be quite difficult. A major milestone in this direction was the paper by Brickell and Davenport [?] who showed that all ideal secret sharing schemes can be obtained from matroids. Not all matroids, however, define ideal schemes [?] so the problem is reduced to classifying those matroids that do. There was little further progress, if any, in this direction.

Several authors attempted to classify all ideal access structures in subclasses of secret sharing schemes. These include access structures defined by graphs [?], weighted threshold access structures [1, 6], hierarchical access structures [6], bipartite and tripartite access structures [15, 16, 5]. While in the classes of bipartite and tripartite access structures the ideal ones were given explicitly, for the case of weighted threshold access structures Beimel et al [1] suggested a new kind of description. Their method uses the operation of composition of access structures first studied by Shapley [19] and later rediscovered by Martin [13]. Under this approach the first task is obtaining a characterisation of indecomposable structures. Beimel et al [1] proved that every ideal indecomposable secret sharing scheme is either disjunctive hierarchical or tripartite. Farras and Padro [6, 7] later gave a more precise classification which was complete (but some access structures that they viewed as indecomposable later appeared to be decomposable).

If a composition of two weighted access structures were again a weighted structure there will not be need to do anything else. However, we will show that this is not true. Since the composition of two weighted access structures may not be again weighted, it is not clear which weighted indecomposable ideal access structures and in which numbers can be

combined to obtain more complex weighted ideal access structures. To answer this question in this paper we undertake a thorough investigation of the operation of composition. We then recap the classification of indecomposable ideal weighted simple games given by [6]. According to it all ideal indecomposable games are either k -out-of- n games or belong to one of the six classes: \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , \mathbf{T}_2 , \mathbf{T}_3 . We show that some of the games in their list are in fact decomposable, and hence arrive at a refined list of all indecomposable ideal weighted simple games.

We investigate which of the games from the refined list can be composed to obtain a new ideal weighted simple game. The result is quite striking; the composition of two indecomposable weighted ideal games is weighted only in two cases: when the first game is a k -out-of- n game, or if the first game is of type \mathbf{B}_2 (from the Farras and Padro list) and the second game is an anti-unanimity game where all players are passers, i.e., players that can win without forming a coalition with other players. This has a major implication for the refinement of Beimel-Tassa-Weinreb-Farras-Padro theorem.

Using the results mentioned above, we show that a game G is an ideal weighted simple game if and only if it is a composition

$$G = H_1 \circ \dots \circ H_s \circ I \circ A_n,$$

where H_i is a k_i -out-of- n_i game for each $i = 1, 2, \dots, s$, A_n is an anti-unanimity game, and I is an indecomposable game of types \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , and \mathbf{T}_3 . Any of these may be absent but A_n may appear only if I is of type \mathbf{B}_2 . The main surprise in this result is that in the decomposition there may be at most one game of types \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , \mathbf{T}_3 .

2 Preliminaries

2.1 Secret Sharing Schemes

Due to lack of space, for preliminaries on secret sharing schemes we send the reader to papers [1, 2, 12, 6, 18, 20].

2.2 Simple Games

The main motivation for this work comes from secret sharing. However, the access structure on the set of users is a *simple game* on that set so we will use game-theoretic terminology.

Definition 1 (von Neumann & Morgenstern, 1944). *A simple game is a pair $G = (P_G, W_G)$, where P_G is a set of players and $W_G \subseteq 2^{P_G}$ is a nonempty set of coalitions which satisfies the monotonicity condition: if $X \in W_G$ and $X \subseteq Y$, then $Y \in W_G$. Coalitions from set W_G are called winning coalitions of G , the remaining ones are called losing.*

A typical example of a simple game is the United Nations Security Council, which consists of five permanent members and 10 nonpermanent. The passage of a resolution requires that all five permanent members vote for it, and also at least nine members in total.

A simple game will be called just a game. The set W_G of winning coalitions of a game G is completely determined by the set W_G^{\min} of its minimal winning coalitions. A player which does not belong to any minimal winning coalitions is called a *dummy*. He can be removed from any winning coalition without making it losing. A player who is contained in every minimal winning coalition is called a *vetoer*. A game with a unique minimal winning coalition is called an *oligarchy*. In an oligarchy every player is either a vetoer or a dummy. A player who alone forms a winning coalition is called a *passer*. A game in which all minimal winning coalitions are singletons is called *anti-oligarchy*. In an anti-oligarchy every player is either a passer or a dummy.

Definition 2. A simple game G is called weighted threshold game if there exist nonnegative weights w_1, \dots, w_n and a real number q , called quota, such that

$$X \in W_G \iff \sum_{i \in X} w_i \geq q. \quad (1)$$

This game is denoted $[q; w_1, \dots, w_n]$. We call such a game simply weighted.

It is easy to see that the United Nation Security Council can be defined in terms of weights as $[39; 7, \dots, 7, 1, \dots, 1]$. In secret sharing weighted threshold access structures were introduced by [18, 2].

For $X \subset P$ we will denote its complement $P \setminus X$ by X^c .

Definition 3. Let $G = (P, W)$ be a simple game and $A \subseteq P$. Let us define subsets

$$W_{sg} = \{X \subseteq A^c \mid X \in W\}, \quad W_{rg} = \{X \subseteq A^c \mid X \cup A \in W\}.$$

Then the game $G_A = (A^c, W_{sg})$ is called a subgame of G and $G^A = (A^c, W_{rg})$ is called a reduced game of G .

The two main concepts of the theory of games that we will need here are as follows.

Given a simple game G on the set of players P we define a relation \succeq_G on P by setting $i \succeq_G j$ if for every set $X \subseteq P$ not containing i and j

$$X \cup \{j\} \in W_G \implies X \cup \{i\} \in W_G. \quad (2)$$

In such case we will say that i is at least as *desirable* (as a coalition partner) as j . In the United Nations Security Council every permanent member will be more desirable than any nonpermanent one. This relation is reflexive and transitive but not always complete (total) (e.g., see [3]). The corresponding equivalence relation on $[n]$ will be denoted \sim_G and the strict desirability relation as \succ_G . We will often omit the subscript G . Any game with complete desirability relation is called *complete*. Any weighted game is complete.

We note that in (2) we can choose X which is minimal with this property in which case $X \cup \{i\}$ will be a minimal winning coalition. Hence the following is true.

Proposition 1. Given a complete simple game G on the set of players P and two players $i, j \in P$, the relation $i \succ_G j$ is equivalent to the existence of a minimal winning coalition X which contains i but not j such that $(X \setminus \{i\}) \cup \{j\}$ is losing.

Proof. Suppose $i \succ_G j$. Then there exist a coalition Y such that $Y \cup \{j\}$ is losing but $Y \cup \{i\}$ is winning. We can take a minimal coalition Y with this property. Then Y is a losing coalition, otherwise $Y \cup \{j\}$ would be also winning. We see now that $X = Y \cup \{i\}$ is winning but becomes losing if any of its elements is removed. It also becomes losing if i is replaced by j . So X is the coalition sought for. The converse is clear due to completeness of G . \square

We recap that a sequence of coalitions

$$\mathcal{T} = (X_1, \dots, X_j; Y_1, \dots, Y_j) \quad (3)$$

is a trading transform [17] if the coalitions X_1, \dots, X_j can be converted into the coalitions Y_1, \dots, Y_j by rearranging players. This latter condition can also be expressed as

$$|\{i : a \in X_i\}| = |\{i : a \in Y_i\}| \quad \text{for all } a \in P.$$

It is worthwhile to note that while in (3) we can consider that no X_i coincides with any of Y_k , it is perfectly possible that the sequence X_1, \dots, X_j has some terms equal, the sequence Y_1, \dots, Y_j can also contain equal terms.

Elgot [4] proved (see also [17]) the following fundamental fact.

Theorem 1. *A game G is a weighted threshold game if for no integer j there exists a trading transform (3) such that all coalitions X_1, \dots, X_j are winning and all Y_1, \dots, Y_j are losing.*

Due to this theorem any trading transform (3) where all coalitions X_1, \dots, X_j are winning and all Y_1, \dots, Y_j are losing is called a *certificate of nonweightedness* [9].

Completeness can also be characterized in terms of trading transforms [17].

Theorem 2. *A game G is complete if no certificate of nonweightedness exists of the form*

$$\mathcal{T} = (X \cup \{x\}, Y \cup \{y\}; X \cup \{y\}, Y \cup \{x\}). \quad (4)$$

We call (4) a *certificate of incompleteness*. This theorem says that completeness is equivalent to the impossibility for two winning coalitions to swap two players and become both losing. This latter property is also called *swap robustness*.

A complete game $G = (P, W)$ can be compactly represented using multisets. All its players are split into equivalence classes of players of equal desirability. If, say, we have m equivalence classes, i.e., $P = P_1 \cup P_2 \cup \dots \cup P_m$ with $|P_i| = n_i$, then we can think that P is the multiset

$$\{1^{n_1}, 2^{n_2}, \dots, m^{n_m}\}.$$

A submultiset $\{1^{\ell_1}, 2^{\ell_2}, \dots, m^{\ell_m}\}$ will then denote the class of coalitions where ℓ_i players come from P_i , $i = 1, \dots, m$. All of them are either winning or all losing. We may enumerate classes so that $1 \succ_G 2 \succ_G \dots \succ_G m$. The game with m classes is called *m-partite*.

If a game G is complete, then we define *shift-minimal* [3] winning coalitions as follows. By a *shift* we mean a replacement of a player of a coalition by a less desirable player which did not belong to it. Formally, given a coalition X , player $p \in X$ and another player $q \notin X$ such that $q \prec_G p$, we say that the coalition $(X \setminus \{p\}) \cup \{q\}$ is obtained from X by a *shift*. A winning coalition X is *shift-minimal* if every coalition strictly contained in it and every coalition obtained from it by a shift are losing. A complete game is fully defined by its shift-minimal winning coalitions.

Example 1 (Unipartite games). *Let $H_{n,k}$ be the game where there are n players and it takes k or more to win. Such games are called k -out-of- n games. Alternatively they can be characterised as the class of complete unipartite games, i.e., the games with a single class of equivalent players. The game $H_{n,n}$ is special and is called the unanimity game on n players. We will denote it as U_n . The game $H_{n,1}$ does not have a name in the literature. We will call it anti-unanimity game and denote A_n .*

Example 2 (Bipartite games). *Here we introduce two important types of bipartite games. A hierarchical disjunctive game $H_{\exists}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$ on a multiset $P = \{1^{n_1}, 2^{n_2}\}$ is defined by the set of winning coalitions*

$$W_{\exists} = \{\{1^{\ell_1}, 2^{\ell_2}\} \mid (\ell_1 \geq k_1) \vee (\ell_1 + \ell_2 \geq k_2)\},$$

where $1 \leq k_1 < k_2$, $k_1 \leq n_1$ and $k_2 - k_1 < n_2$. A hierarchical conjunctive game $H_{\forall}(\mathbf{n}, \mathbf{k})$ with $\mathbf{n} = (n_1, n_2)$ and $\mathbf{k} = (k_1, k_2)$ on a multiset $P = \{1^{n_1}, 2^{n_2}\}$ is defined by the set of winning coalitions

$$W_{\forall} = \{\{1^{\ell_1}, 2^{\ell_2}\} \mid (\ell_1 \geq k_1) \wedge (\ell_1 + \ell_2 \geq k_2)\},$$

where $1 \leq k_1 \leq k_2$, $k_1 \leq n_1$ and $k_2 - k_1 < n_2$. In both cases, if the restrictions on \mathbf{n} and \mathbf{k} are not satisfied the game becomes unipartite [8]).

Example 3 (Tripartite games). Here we introduce two types of tripartite games. Let $\mathbf{n} = (n_1, n_2, n_3)$ and $\mathbf{k} = (k_1, k_2, k_3)$, where n_1, n_2, n_3 and k_1, k_2, k_3 are positive integers. The game $\Delta_1(\mathbf{n}, \mathbf{k})$ is defined on the multiset $P = \{1^{n_1}, 2^{n_2}, 3^{n_3}\}$ with the set of winning coalitions

$$\{\{1^{\ell_1}, 2^{\ell_2}, 3^{\ell_3}\} \mid (\ell_1 \geq k_1) \vee [(\ell_1 + \ell_2 \geq k_2) \wedge (\ell_1 + \ell_2 + \ell_3 \geq k_3)]\},$$

where

$$k_1 < k_3, \quad k_2 < k_3, \quad n_1 \geq k_1, \quad n_2 > k_2 - k_1 \quad \text{and} \quad n_3 > k_3 - k_2. \quad (5)$$

These, in particular, imply $n_1 + n_2 \geq k_2$.

The game $\Delta_2(\mathbf{n}, \mathbf{k})$ is for the case when $n_2 \leq k_2 - k_1$, and it is defined on the multiset $P = \{1^{n_1}, 2^{n_2}, 3^{n_3}\}$ with the set of winning coalitions

$$\{\{1^{\ell_1}, 2^{\ell_2}, 3^{\ell_3}\} \mid (\ell_1 + \ell_2 \geq k_2) \vee [(\ell_1 \geq k_1) \wedge (\ell_1 + \ell_2 + \ell_3 \geq k_3)]\}.$$

where

$$k_1 < k_2 < k_3, \quad n_1 + n_2 \geq k_2, \quad n_3 > k_3 - k_2, \quad \text{and} \quad n_2 + n_3 > k_3 - k_1. \quad (6)$$

These conditions, in particular, imply $n_1 \geq k_1$ and $n_3 \geq 2$.

In both cases, if the restrictions on \mathbf{n} and \mathbf{k} are not satisfied the game either contains dummies or becomes 2-partite or even unipartite (see a justification of this claim in the appendix).

The games in these three examples play a crucial role in classification of ideal weighted secret sharing schemes [1, 6].

3 The Operation of Composition of Games

The most general type of compositions of simple games was defined by [19]. We need a very partial case of that concept here, which is in the context of secret sharing, was introduced by [13].

Definition 4. Let G and H be two games defined on disjoint sets of players and $g \in P_G$. We define the composition game $C = G \circ_g H$ by defining $P_C = (P_G \setminus \{g\}) \cup P_H$ and

$$W_C = \{X \subseteq P_C \mid X_G \in W_G \text{ or } (X_G \cup \{g\}) \in W_G \text{ and } X_H \in W_H\},$$

where $X_G = X \cap P_G$ and $X_H = X \cap P_H$.

This is a substitution of a single element g of G by H . All winning compositions in G not containing g remain winning in C . If a winning coalition of G contained g , then it remains winning in C if g is replaced with a winning coalition of H .

Definition 5. A game G is said to be indecomposable if there does not exist two games H and K and $h \in P_H$ such that $\min(|H|, |K|) > 1$ and $G \cong H \circ_h K$. Otherwise, it is called decomposable.

Example 4. Let $G = (P, W)$ be a simple game and $A \subseteq P$ be the set of all vetoers in this game. Let $|A| = m$. Then $G \cong U_{m+1} \circ_u G^A$, where u is any player of U_{m+1} . So any game with vetoers is decomposable.

Example 5. Let $G = (P, W)$ be a simple game and $A \subseteq P$ be the set of all passers in this game. Let $|A| = m$. Then $G \cong A_{m+1} \circ_a G_A$, where a is any player of A_{m+1} . So any game with passers is decomposable.

Suppose $G = (P, W)$ and $G' = (P', W')$ be two games and $\sigma: P \rightarrow P'$ is a bijection. We say that σ is an isomorphism of G and G' , and denote this as $G \cong G'$, if $X \in W$ if and only if $\sigma(X) \in W'$.

It is easy to see that if $|H| = 1$, then $H \circ_h K \cong K$ and, if $|K| = 1$, then $H \circ_h K \cong H$.

Proposition 2. *Let G, H be two games defined on disjoint sets of players and $g \in P_G$. Then*

$$W_{G \circ_g H}^{\min} = \{X \mid X \in W_G^{\min} \text{ and } g \notin X\} \cup \{X \cup Y \mid X \cup \{g\} \in W_G^{\min} \text{ and } Y \in W_H^{\min} \text{ with } g \notin X\}.$$

Proof. Follows directly from the definition. \square

Proposition 3. *Let G, H, K be three games defined on disjoint sets of players and $g \in P_G$, $h \in P_H$. Then*

$$(G \circ_g H) \circ_h K \cong G \circ_g (H \circ_h K),$$

that is the two compositions are isomorphic.

Proof. Straightforward. \square

Proposition 4. *Let G, H be two games defined on disjoint sets of players. Then $G \circ_g H$ has no dummies if and only if both G and H have no dummies.*

Proof. Straightforward. \square

4 Decompositions of Weighted Games and Ideal Games

The following result was proved in [1] and was a basis for this new type of description.

Proposition 5. *Let $C = G \circ_g H$ be a decomposition of a game C over an element $g \in P_G$, which is not a dummy. Then, C is ideal if and only if G and H are also ideal.*

Suppose we have a class of games \mathcal{C} such that if the composition $G \circ_g H$ belongs to \mathcal{C} , then both G and H belong to \mathcal{C} . This proposition means that in any class of games \mathcal{C} with the above property we may represent any game as a composition of indecomposable ideal games also belonging to \mathcal{C} . The class of weighted games as the following lemma shows satisfies the above property, Hence, if we would like to describe ideal games in the class of weighted games we should look at indecomposable weighted games first.

Lemma 1. *Let $C = G \circ_g H$ be a decomposition of a game C into two games G and H over an element $g \in P_G$, which is not dummy. Then, if C is weighted, then G and H are weighted.*

Proof. A simple proof using trading transforms is relegated to the appendix. \square

Corollary 1. *Every weighted game is a composition of indecomposable weighted games.¹*

The converse is however not true. As we will see in the next section, the composition $C = G \circ_g H$ of two weighted games G and H is seldom weighted. Thus we will pay attention to those cases where compositions are weighted. One of those which we will now consider is when G is a k -out-of- n game. In this case all players of G are equivalent and we will often omit g and write the composition as $C = G \circ H$.

¹As usual we assume that if a game G is indecomposable, its decomposition into a composition of indecomposable games is $G = G$, i.e., trivial.

Theorem 3. *Let $H = H_{n,k}$ be a k -out-of- n game and G is a weighted simple game. Then $C = H \circ G$ is also a weighted game.*

Proof. Let X_1, \dots, X_m be winning and Y_1, \dots, Y_m be losing coalitions of C such that

$$(X_1, \dots, X_m; Y_1, \dots, Y_m)$$

is a trading transform. Without loss of generality we may assume that X_1, \dots, X_m are minimal winning coalitions. Let $U_i = X_i \cap H$, then U_i is either winning in H or winning with h , hence $|U_i| = k$ or $|U_i| = k - 1$. If for a single i we had $|U_i| = k$, then all of the sets Y_1, \dots, Y_m could not be losing since at least one of them would contain k elements from H . Thus $|U_i| = k - 1$ for all i . In this case we have $X_i = U_i \cup S_i$, where S_i is winning in G . Let $Y_i = V_i \cup T_i$, where $V_i \subseteq H$ and $T_i \subseteq G$. Since all coalitions Y_1, \dots, Y_m are losing in C , we get $|V_i| = k - 1$ which implies that all T_i are losing in G . But now we have obtained a trading transform $(S_1, \dots, S_m; T_1, \dots, T_m)$ in G such that all S_i are winning and all T_i are losing. This contradicts to G being weighted. \square

5 Compositions of complete games

We will start with the following observation. It says that if $g \in P_G$ is not the least desirable player of G , then the composition $G \circ_g H$ is almost never swap robust, hence is almost never complete.

Lemma 2. *Let G, H be two games on disjoint sets of players and H is neither a oligarchy nor an anti-oligarchy. If for two elements $g, g' \in P_G$ we have $g \succ g'$ and g' is not a dummy, then $G \circ_g H$ is not complete.*

This lemma shows that if a composition $G \circ_g H$ of two weighted games is weighted, then almost always g is one of the least desirable players of G . Theorem 4 shows that If G has no dummies and we compose two weighted games over the weakest player of the first game, the result will be always complete, however, as is shown in Subsection 12.3, it will not always be weighted.

Theorem 4. *Let G and H be two complete games, $g \in G$ be one of the least desirable players in G but not a dummy. Then for the game $C = G \circ_g H$*

(i) *for $x, y \in P_G \setminus \{g\}$ it holds that $x \succeq_G y$ if and only if $x \succeq_C y$.*

(ii) *for $x, y \in P_H$ it holds that $x \succeq_H y$ if and only if $x \succeq_C y$.*

(iii) *for $x \in P_G \setminus \{g\}$ and $y \in P_H$, then $x \succeq_C y$; if y is not a passer or vetoer in H , then $x \succ_C y$.*

In particular, C is complete.

Proof. (i) Suppose $x \succeq_G y$ but not $x \succeq_C y$. Then there exist $Z \subseteq C$ such that $Z \cup \{y\} \in W_C$ but $Z \cup \{x\} \notin W_C$. We can take Z minimal with this property. Consider $Z' = Z \cap P_G$. Then either $Z' \cup \{y\}$ is winning in G , or else $Z' \cup \{y\}$ is losing in G but $Z' \cup \{y\} \cup \{g\}$ is winning in G . In the latter case $Z \cap P_H \in W_H$. In the first case, since $x \succeq_G y$, we have also $Z' \cup \{x\} \in W_G$, which contradicts $Z \cup \{x\} \notin W_C$. Similarly, in the second case we have $Z' \cup \{x\} \cup \{g\} \in W_G$ and since $Z \cap P_H \in W_H$, this contradicts $Z \cup \{x\} \notin W_C$ also. Hence $x \succeq_C y$.

If $x \succ_G y$, then there exists $S \subseteq P_G$ such that $S \cap \{x, y\} = \emptyset$ and $S \cup \{x\} \in W_G$ but $S \cup \{y\} \notin W_G$. We may assume S is minimal with this property. If S does not contain g , then

S is also winning in C and $x \succ_C y$, so we are done. (ii) This case is similar to the previous one. If S contains g , then consider any winning coalition K in H . Then $(S \setminus \{g\}) \cup \{x\} \cup K$ is winning in C while $(S \setminus \{g\}) \cup \{y\} \cup K$ is losing in C . Hence $x \succ_C y$.

(iii) We have $x \succeq_G g$ since g is from the least desirable class in G . Let us consider a coalition $Z \subset C$ such that $Z \cap \{x, y\} = \emptyset$, and suppose there exists $Z \cup \{y\} \in W_C$ but $Z \cup \{x\} \notin W_C$. Then Z must be losing in C , and hence $Z \cap P_G$ cannot be winning in G , but $Z \cap P_G \cup \{g\}$ must be winning in G . However, since $x \succeq_G g$, the coalition $Z \cap P_G \cup \{x\}$ is also winning in G . But then $Z \cup \{x\}$ is winning in C , a contradiction. This shows that if $Z \cup \{y\}$ is winning in C , then $Z \cup \{x\}$ is also winning in C , meaning $x \succeq_C y$. Thus C is a complete game.

Moreover, suppose that y is not a passer or a vetoer in H , we will show that $x \succ_C y$. Since g is not a dummy, then x is not a dummy either. Let X be a minimal winning coalition of G containing x . If $g \notin X$, then X is also winning in C . However, $X \setminus \{x\} \cup \{y\}$ is losing in C , since y is not a passer in H . Thus it is not true that $y \succeq_C x$ in this case. If $g \in X$, then consider a winning coalition Y in H not containing y (this is possible since y is not a vetoer in H). Then $X \setminus \{g\} \cup Y \in W_C$ but $X \setminus \{x, g\} \cup \{y\} \cup Y \notin W_C$, since $X \setminus \{x\}$ is not winning in G . Whence it is not true that $y \succeq_C x$ in this case as well. Thus $x \succ_C y$ in case y is neither a passer nor a vetoer in H . \square

6 Indecomposable unipartite games and uniqueness of some decompositions

Theorem 5. *A game $H_{n,k}$ for $n \neq k \neq 1$ is indecomposable.*

Proof. Suppose $H_{n,k}$ is decomposable into $H_{n,k} = K \circ_g L$, where $K = (P_K, W_K), L = (P_L, W_L)$ with $n_1 = |P_K| \geq 2$ and $n_2 = |P_L| \geq 2$. If g is a passer in K , then it is the only passer, otherwise if there is another passer g' in K , then $\{g'\}$ is winning in the composition, contradicting $k \neq 1$.

We will firstly show that $n_2 < k$. Suppose that $n_2 \geq k$, and choose a player $h \in P_K$ different from g . Consider a coalition X containing k players from P_L , then X is winning in the composition without having any players from K , hence g is a passer in K . It is also the case that X is a minimal winning coalition in L . Now replace a player x in X from P_L with h . The resulting coalition, although it has k players, is losing in the composition, because h is not a passer in K , and $k - 1$ players from P_L are losing in L . This contradiction shows that $k > n_2$.

The latter restriction implies $|P_K \setminus \{g\}| = n - n_2 > k - n_2 > 0$. Let us choose any coalition Z in $P_K \setminus \{g\}$ with $k - n_2$ players. If it does not win in K with g , then $Z \cup P_L$ is also losing despite having k players in total, contradiction. Suppose $Z \cup \{g\}$ is winning in K . Then $|Z \cup \{g\}| = k - n_2 + 1 < k$ and replacing g with any element x of L does not result in a winning coalition. Hence all elements of L are not passers and, in particular, $n_2 > 1$. Since $|P_K \setminus \{g\}| > k - n_2$, we can choose $k - n_2 + 1$ elements from $P_K \setminus \{g\}$ and complement it with any $n_2 - 1$ elements from L and get a winning coalition. This shows that any $n_2 - 1$ elements form a winning coalition in L hence L is not a unanimity game and no element of it is a vetoer. By Theorem 4 (iii) we get $x \succ y$ for any $x \in P_K \setminus \{g\}$ and any $y \in L$. This however contradicts to the fact that $H_{n,k}$ is unipartite. \square

If the first component of the composition is a k -out-of- n game, there is a uniqueness of decomposition.

Theorem 6. *Let H_{n_1, k_1} and H_{n_2, k_2} be two k -out-of- n games which are not unanimity games. Then, if $G = H_{n_1, k_1} \circ G_1 = H_{n_2, k_2} \circ G_2$, with G_1 and G_2 having no passers, then*

$n_1 = n_2$, $k_1 = k_2$ and $G_1 = G_2$. If $G = U_{n_1} \circ G_1 = U_{n_2} \circ G_2$ and G_1 and G_2 does not have vetoers, then $n_1 = n_2$ and $G_1 = G_2$.

Proof. Suppose that we know that $G = H \circ G_1$, where H is a k -out-of- n game but not a unanimity game. Then all winning coalitions in G of smallest cardinality have k players, so k in this case can be recovered unambiguously.

If G_1 does not have passers, then n can be also recovered since the set of all players that participate in winning coalitions of size k will have cardinality $n - 1$. So there cannot exist two decompositions $G = H_{n_1, k_1} \circ G_1$ and $G = H_{n_2, k_2} \circ G_2$ of G , where $k_1 \neq k_2$ with $k_1 \neq n_1$ and $k_2 \neq n_2$.

Suppose now $G = U \circ G_1$, where U is a unanimity game. Due to Example 4 if G_1 does not have vetoers, then U consists of all vetoers of G and uniquely recoverable. \square

7 Indecomposable Ideal Weighted Simple Games

The following theorem was proved in [6] and is of a major importance to us.

Theorem 7 (Farràs-Padró, 2010). *Any indecomposable ideal weighted simple game belongs to one of the seven following types:*

$\tilde{\mathbf{H}}$: *Simple majority or k -out-of- n games.*

$\tilde{\mathbf{B}}_1$: *Hierarchical conjunctive games $H_{\forall}(n, k)$ with $\mathbf{n} = (n_1, n_2)$, $\mathbf{k} = (k_1, k_2)$, where $k_1 < n_1$ and $k_2 - k_1 = n_2 - 1 > 0$. Such games have the only shift-minimal winning coalition $\{1^{k_1}, 2^{k_2 - k_1}\}$.*

\mathbf{B}_2 : *Hierarchical disjunctive games $H_{\exists}(n, k)$ with $\mathbf{n} = (n_1, n_2)$, $\mathbf{k} = (k_1, k_2)$, where $1 < k_1 \leq n_1$, $k_2 \leq n_2$, and $k_2 = k_1 + 1$. The shift-minimal winning coalitions have the forms $\{1^{k_1}\}$ and $\{2^{k_2}\}$.*

\mathbf{B}_3 : *Hierarchical disjunctive games $H_{\exists}(n, k)$ with $\mathbf{n} = (n_1, n_2)$, $\mathbf{k} = (k_1, k_2)$, where $k_1 \leq n_1$, $k_2 > n_2 > 2$ and $k_2 = k_1 + 1$. The shift-minimal winning coalitions have the forms $\{1^{k_1}\}$ and $\{1^{k_2 - n_2}, 2^{n_2}\}$.*

\mathbf{T}_1 : *Tripartite games $\Delta_1(\mathbf{n}, \mathbf{k})$ with $k_1 > 1$, $k_2 < n_2$, $k_3 = k_1 + 1$ and $n_3 = k_3 - k_2 + 1 > 2$. It has two types of shift-minimal winning coalitions: $\{1^{k_1}\}$ and $\{2^{k_2}, 3^{k_3 - k_2}\}$. It follows from (5) that $k_1 \leq n_1$ and $k_3 - k_2 \leq n_3$.*

\mathbf{T}_2 : *Tripartite games $\Delta_1(\mathbf{n}, \mathbf{k})$ with $n_3 = k_3 - k_2 + 1 > 2$ and $k_3 = k_1 + 1$. It has two types of shift-minimal winning coalitions: $\{1^{k_1}\}$ and $\{1^{k_2 - n_2}, 2^{n_2}, 3^{k_3 - k_2}\}$. It follows from (5) that $k_1 \leq n_1$, $k_2 - n_2 \leq k_1$, and $k_3 - k_2 \leq n_3$.*

\mathbf{T}_3 : *Tripartite games $\Delta_2(\mathbf{n}, \mathbf{k})$ with $k_3 - k_1 = n_2 + n_3 - 1$ and $k_3 = k_2 + 1$ and $k_2 - n_2 > k_1$, $n_3 > 1$. It has two types of shift-minimal winning coalitions $\{1^{k_2 - n_2}, 2^{n_2}\}$ and $\{1^{k_1}, 2^{k_3 - k_1 - n_3}, 3^{n_3}\}$ (the case when $k_3 - k_1 = n_3$ and $n_2 = 1$ is not excluded). It follows from (6) that $k_1 \leq n_1$, $k_2 - n_2 \leq n_1$, and $k_3 - k_1 - n_3 < n_2$.*

Farras and Padro [7] wrote these families more compactly but equivalently. However, we found it more convenient to use their earlier classification. The list above contains some decomposable games as we will now show.

Proposition 6. *The game of type \mathbf{B}_1 for $k_2 - k_1 = n_2 - 1 = 1$ is decomposable.*

Proof. The decomposition is as follows: Assume $k_2 - k_1 = n_2 - 1 = 1$, so $n_2 = 2$ and $k_2 = k_1 + 1$, then we have $\mathbf{k} = (k_1, k_1 + 1)$, $\mathbf{n} = (n_1, 2)$, and the only shift-minimal winning coalition here is $\{1^{k_1}, 2\}$. Let the first game $G = (P_G, W_G)$, be unipartite with $P_G = \{1^{n_1+1}\}$, $W_G = \{1^{k_1+1}\}$, and let the second game be $H = (P_H, W_H)$, $P_H = \{2^2\}$, $W_H = \{2\}$. Then the composition $G \circ_1 H$ over a player $1 \in P_G$ gives two minimal winning coalitions $\{1^{k_1+1}\}$ and $\{1^{k_1}, 2\}$, of which only $\{1^{k_1}, 2\}$ is shift-minimal. Hence the composition is of type \mathbf{B}_1 . This proves that a game of type \mathbf{B}_1 is decomposable in this case. \square

Proposition 7. *The unanimity games U_n and anti-unanimity A_n for $n > 2$ are decomposable. U_2 and A_2 are indecomposable.*

Proof. We note that

$$U_n \circ U_m \cong U_{n+m-1}$$

for any $u \in U_n$. In particular, the only indecomposable unanimity game is U_2 . Similarly,

$$A_n \circ A_m \cong A_{n+m-1}$$

for any $a \in A_n$ with the only indecomposable anti-unanimity game is A_2 . \square

Proposition 8. *All games of type \mathbf{T}_2 are decomposable.*

Proof. Let $\Delta = \Delta_1(\mathbf{n}, \mathbf{k})$ be of type \mathbf{T}_2 . Then we have the following decomposition for it. The first game will be $G = (P_G, W_G)$, which is bipartite with the multiset representation on $\{1^{n_1}, 2^{n_2+1}\}$ and shift-minimal winning coalitions of types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2+1}\}$. The second game will be $(k_3 - k_2)$ -out-of- n_3 game $H = (P_H, W_H)$, with the multiset representation on $\bar{P}_H = \{3^{n_3}\}$ and shift-minimal winning coalitions of type $\{3^{k_3-k_2}\}$. The composition is over a player $p \in P_G$ from level 2. Then we can see that $G \circ_p H$ has shift-minimal winning coalitions of types $\{1^{k_1}\}$ and $\{1^{k_2-n_2}, 2^{n_2}, 3^{k_3-k_2}\}$, hence is exactly Δ . \square

We now refine classes $\tilde{\mathbf{H}}$ and $\tilde{\mathbf{B}}_1$ as follows:

H: Games of this type are A_2, U_2 and $H_{n,k}$, where $1 < k < n$.

B₁: Hierarchical conjunctive games $H_{\vee}(n, k)$ with $\mathbf{n} = (n_1, n_2)$, $\mathbf{k} = (k_1, k_2)$, where $k_1 < n_1$ and $k_2 - k_1 = n_2 - 1 > 1$.

The following of Theorem 7, is now an if-and-only-if statement.

Theorem 8. *A game is ideal weighted and indecomposable if and only if it belongs to one of the following types: $\mathbf{H}, \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{T}_1, \mathbf{T}_3$.*

Proof. Due to Theorem 7 and Propositions 6-8 all that remains to show is that the remaining cases are indecomposable. We leave this routine work to the reader. \square

Let us compare this theorem with Theorem 7. We narrowed the class \mathbf{H} , we excluded the case $n_2 = 2$ in \mathbf{B}_1 and removed class \mathbf{T}_2 .

8 Compositions of indecomposable games

The key result that will lead us to the main theorem of this paper is the following.

Theorem 9. *Let G be a game with no dummies which has a nontrivial decomposition $G = G_1 \circ_g G_2$, such that G_1 and G_2 are both ideal and weighted, and G_1 is indecomposable. Then G is ideal weighted if and only if either*

(i) G_1 is of type \mathbf{H} , or

(ii) G_1 is of type \mathbf{B}_2 and G_2 is A_n and the composition is over a player g of level 2 of G_1 .

We will prove it in several steps. Firstly, we will consider all cases when g is from the least desirable level of G_1 . Secondly, in Appendix, we will deal with the hypothetical remaining cases. This is unfortunately needed since Lemma 2 still leaves a possibility that for some special cases of G_2 element g may not be in the least desirable class of G_1 .

We note that case (i) of Theorem 9 was treated in Theorem 3. Let us deal with case (ii).

Proposition 9. *Let $G_1 = (P_1, W_1)$ be a weighted simple game of type \mathbf{B}_2 , g is a player from level 2 of P_1 , and G_2 is A_n , then $G = G_1 \circ_g G_2$ is a weighted simple game.*

Proof. Since g is a player from level 2 of P_1 , then G is a complete game by Theorem 4. Also, recall that shift-minimal winning coalitions of a game of type \mathbf{B}_2 are $\{1^{k_1}\}$ and $\{2^{k_1+1}\}$. We shall prove weightedness of G by showing that it cannot have a certificate of nonweightedness. In the composition, in the multiset notation, G has the following shift-minimal winning coalitions $\{1^{k_1}, \{2^{k_1}, 3\}$. So all shift-minimal winning coalitions have k_1 players from $P_1 \setminus \{g\}$. Also, since G_1 has two thresholds k_1 and k_2 such that $k_2 = k_1 + 1$, then any coalition containing more than k_1 players from $P_1 \setminus \{g\}$ is winning in G_1 , and hence winning in G . Suppose now towards a contradiction that G has the following certificate of nonweightedness

$$(X_1, \dots, X_n; Y_1, \dots, Y_n), \quad (7)$$

where X_1, \dots, X_n are shift-minimal winning coalitions and Y_1, \dots, Y_n are losing coalitions in G . Let the set of players of A_n be P_{A_n} . It is easy to see that at least one of the coalitions X_1, \dots, X_n in (7) is not of the type $\{1^{k_1}\}$, so at least one of these winning coalitions has a player from the third level, i.e. from A_n . But since each shift-minimal winning coalition in (7) has k_1 players from $P_1 \setminus \{g\}$, then each losing coalition Y_1, \dots, Y_n in (7) also has k_1 players from $P_1 \setminus \{g\}$ (if it has more than k_1 then it is winning). Moreover, at least one coalition from Y_1, \dots, Y_n , say Y_1 , has at least one player from P_{A_n} . It follows that $(Y_1 \cap P_1) \cup \{g\} \in W_1$ and $Y_1 \cap P_{A_n}$ is winning in A_n . Hence Y_1 is winning in G , contradiction. Therefore no such certificate can exist. \square

The analysis of the remaining of compositions $G = G_1 \circ G_2$ in terms of G_1 , where the composition is over a player from the least desirable level of G_1 , show that none of them are weighted (see the appendix).

9 The Main Theorem

All previous results combined give us the main theorem:

Theorem 10. *G is an ideal weighted simple game without dummies if and only if it is a composition*

$$G = H_1 \circ \dots \circ H_s \circ I \circ_g A_n \quad (s \geq 0); \quad (8)$$

where H_i is an indecomposable game of type \mathbf{H} for each $i = 1, \dots, s$. Also, I , which is allowed to be absent, is an indecomposable game of types $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{T}_1$ and \mathbf{T}_3 , and A_n is the anti-unanimity game on n players. Moreover, A_n can be present only if I is either absent or it is of type \mathbf{B}_2 ; in the latter case the composition $I \circ A_n$ is over a player g of the least desirable level of I . Also, the above decomposition is unique.

The following proposition will be useful to show the uniqueness of the decomposition of an ideal weighted game.

Proposition 10. *Let H be a game of type \mathbf{H} , B be a game of type \mathbf{B}_2 with b being a player from level 2 of B , G be an ideal weighted simple game, and A_n be an anti-unanimity game. Then $H \circ G \not\cong B \circ_b A_n$.*

Proof. We note that by Theorem 4 both compositions are complete. Recall that isomorphisms preserve Isbell's desirability relation [3,]. An isomorphism preserves completeness and maps shift-minimal winning coalitions of a complete game onto shift-minimal winning coalitions of another game.

Let $H = H_{k,n}$. Consider first the composition $H \circ G$. Any minimal winning coalition in this composition will have either k or $k - 1$ players from the most desirable level.

Now consider $B \circ_b A_n$. Let the two types of shift-minimal winning coalitions of B be of the forms $\{1^\ell\}$ and $\{2^{\ell+1}\}$, then there will be a minimal winning coalition in $B \circ_b A_n$ which has ℓ players from the second most desirable level and an element of level 3 with no players of level 1. The two games therefore cannot be isomorphic. \square

Proof of Theorem 10. This proof is now easy since the main work has been done in Theorem 9. Either G is decomposable or not. If it is not, then by Theorem 8 it is either of type \mathbf{H} or one of the indecomposable games of types \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , and \mathbf{T}_3 . So the theorem is trivially true. Suppose now that G is decomposable, so $G = G_1 \circ G_2$. Then by Theorem 9 there are only two possibilities:

- (i) G_1 is of type \mathbf{H} ;
- (ii) G_1 is of type \mathbf{B}_2 , and also $G_2 = A_n$ such that the composition is over a player of level 2 of G_1 .

By Proposition 10 these two cases are mutually exclusive. Suppose we have the case (i). By Theorem 6 G_1 is uniquely defined and we can apply the induction hypothesis to G_2 . It is also easy to see that in the second case G_1 and G_2 are uniquely defined. \square

We finally note that the absence of dummies in access structures is normally implicitly assumed in secret sharing. It is easy to add them and give meaningless shares anyway.

10 Conclusion and Further Research

Game-theoretic techniques proved to be useful in characterisation of secret sharing schemes. Using the machinery of simple games, this paper provides a complete characterisation of weighted ideal simple games in terms of the operation of composition of games. The next step would be to extend this characterisation to the class of roughly weighted simple games [9]. Since hierarchical simple games are always ideal, the first step towards this goal has been made in [11] where all hierarchical roughly weighted games were characterised. Hameed [10] constructed a four-partite roughly weighted ideal simple game but there is a hypothesis that there do not exist five-partite ones.

There are interesting algorithmic questions related to the main result of this paper. It would be interesting to estimate the complexity of the determination of whether or not a particular game is indecomposable and finding a decomposition of it is decomposable.

11 Acknowledgements

The authors thank Carles Padro for a number of useful discussions. We are very grateful to Sascha Kurz for a very useful feedback on the early draft of this paper. We also thank anonymous referees for useful comments and suggestions.

References

- [1] A. Beimel, T. Tassa, and E. Weinreb. Characterizing Ideal Weighted Threshold Secret Sharing. In: *Theory of Cryptography*. Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Volume 3378/2005: 600–619, 2005.
- [2] G.R. Blakley. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference* 48: 313–317, 1979.
- [3] F. Carreras and J. Freixas. (1996) Complete simple games. *Mathematical Social Sciences*, 32(2):139–155.
- [4] C.C. Elgot. Truth Functions Realizable by Single Threshold Organs, *Proc. of the Second Annual Symposium on Switching Circuit Theory and Logical Design*, 225–245, 1961.
- [5] O. Farràs, J. Martí-Farré, and C. Padró. Ideal multipartite secret sharing schemes. *Journal of Cryptology*, 25, 434–463, 2012.
- [6] O. Farràs, and C. Padró. Ideal hierarchical secret sharing schemes. In D. Micciancio (Ed.), *Theory of cryptography* (Vol. 5978, p. 219–236). Springer Berlin / Heidelberg, 2010.
- [7] O. Farràs, and C. Padró. Ideal hierarchical secret sharing schemes. *IEEE Transactions on Information Theory*, 58(5), 3273–3286, 2012.
- [8] T. Gvozdeva, A. Hameed, and A. Slinko. Weightedness and structural characterization of hierarchical simple games. *Mathematical Social Sciences*, 65(3), 181–189, 2013.
- [9] T. Gvozdeva and A. Slinko. Weighted and Roughly Weighted Simple Games, *Mathematical Social Sciences*, 61(1), 20–30, 2011.
- [10] A. Hameed, Simple Games with Applications to Secret Sharing Schemes. PhD Thesis. The University of Auckland, 2013.
- [11] A. Hameed and A. Slinko. Roughly Weighted Hierarchical Simple Games (10 May, 2012), arXiv:1205.2152v1 [math.CO] .
- [12] E.D. Karnin, J.W. Greene, and M.E. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1), 35–41, 1983.
- [13] K. Martin. New secret sharing schemes from old. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 14, 65–77, 1993.
- [14] J. von Neumann, and O. Morgenstern. *Theory of games and economic behavior*. Princeton University Press. 1944.
- [15] C. Padró, and G. Sáez. Secret sharing schemes with bipartite access structure. In K. Nyberg (Ed.), *Advances in Cryptology Eurocrypt98* (Vol. 1403, p. 500–511). Springer Berlin / Heidelberg, 1998.
- [16] C. Padró, and G. Sáez. Correction to Secret sharing schemes with bipartite access structure. *IEEE Transactions on Information Theory*, 50(6), 1373, 2004.
- [17] A.D. Taylor and W.S. Zwicker. *Simple games*. Princeton University Press. Princeton. NJ, 1999.
- [18] A. Shamir. How to share a secret. *Commun. ACM* , 22 , 612–613, 1979.

- [19] L.S. Shapley. Simple Games: An Outline of the Descriptive Theory. *Behavioral Science* 7: 59–66, 1962.
- [20] D. Stinson. An explication of secret sharing schemes. *Design Code Cryptogr.*, 2, 357–390, 1992.

Ali Hameed
 Department of Mathematics
 Private Bag 92019, Auckland Mail Centre
 University of Auckland
 Auckland 1142, NEW ZEALAND
 Email: aham002@aucklanduni.ac.nz

Arkadii Slinko
 Department of Mathematics
 Private Bag 92019, Auckland Mail Centre
 University of Auckland
 Auckland 1142, NEW ZEALAND
 Email: slinko@math.auckland.ac.nz

12 Appendix

12.1 A canonical representation of Δ_1 and Δ_2 .

Proposition 11. *The game $\Delta_1(\mathbf{n}, \mathbf{k})$ is tripartite game without dummies if and only if conditions (5) are satisfied.*

Proof. It is easy to see from the definition that this game is complete and $1 \succeq_G 2 \succeq_G 3$. Suppose we actually have $1 \succ_G 2 \succ_G 3$ so that the game is tripartite. If the condition $k_1 \leq n_1$ is not satisfied the condition $\ell_1 \geq k_1$ has no solution and 1 becomes equivalent to 2. So we assume $k_1 \leq n_1$. If $k_2 \geq k_3$, then the condition $\ell_1 + \ell_2 \geq k_2$ is redundant which implies $2 \sim 3$ and the game is bipartite so we assume $k_2 < k_3$. If $k_1 \geq k_3$, then the coalition $\ell_1 + \ell_2 + \ell_3 \geq k_3$ is redundant and 3 is a dummy. Hence we assume $k_1 < k_3$. If we only had $n_2 \leq k_2 - k_1$, then $\ell_1 + \ell_2 \geq k_2$ can be satisfied only if $\ell_1 \geq k_1$ is satisfied. So in this case $\{1^{k_1}\}$ is the only minimal winning coalition, which implies $2 \sim 3$. So $n_2 > k_2 - k_1$. Finally, if $n_3 > k_3 - k_2$ is not satisfied, then $\ell_1 + \ell_2 + \ell_3 \geq k_3$ implies $\ell_1 + \ell_2 \geq k_2$, in which case the minimal winning coalition must satisfy either $\ell_1 = k_1$ or $\ell_1 + \ell_2 + \ell_3 = k_3$. We get in this case $2 \sim 3$, which is impossible. Hence if $\Delta_1(\mathbf{n}, \mathbf{k})$ is tripartite and has no dummies, the conditions (5) are satisfied.

On the other hand, if (5) are satisfied, then the game has two shift-minimal winning coalitions $\{1^{k_1}\}$ and either $\{2^{k_2}, 3^{k_3-k_2}\}$ in case $k_2 \leq n_2$ or $\{1^{k_2-n_2}, 2^{n_2}, 3^{k_3-k_2}\}$ in case $k_2 > n_2$. In both cases $1 \succ 2 \succ 3$ by Proposition 1. \square

Proposition 12. *The game $\Delta_2(\mathbf{n}, \mathbf{k})$ is tripartite game without dummies if and only if conditions (6) are satisfied.*

Proof. Suppose $\Delta_2(\mathbf{n}, \mathbf{k})$ is tripartite. Like in Proposition 11 we find that $k_1 < k_3$ and $k_2 < k_3$. However, we also know that $k_2 - k_1 \geq n_2 > 0$. Hence we assume $k_1 < k_2 < k_3$. If $n_1 + n_2 \geq k_2$ is not satisfied, then $\ell_1 + \ell_2 \geq k_2$ is ineffectual and $2 \sim 3$. So we assume $n_1 + n_2 \geq k_2$. In this case we have a shift-minimal winning coalition $C = \{1^{k_2-n_2}, 2^{n_2}\}$ and secures that $2 \succ 3$ (as $k_2 < k_3$). If $n_3 > k_3 - k_2$ is not satisfied, then $\ell_1 + \ell_2 + \ell_3 \geq k_3$ is redundant and 3 is a dummy. Since $k_3 > k_2$ we have $n_3 \geq k_3 - k_2 + 1 \geq 2$. Since $\Delta_2(\mathbf{n}, \mathbf{k})$ is defined for the case $n_2 \leq k_2 - k_1$, we have $k_1 \leq k_2 - n_2 \leq n_1$ and $n_1 \geq k_1$ follows.

Now, if the coalitions $\{1^{k_1}\}$ and $\{2^{k_3-k_1-n_3+1}\}$ exist, then a replacement of 1 with 2 in a winning coalition $\{1^{k_1-1}, 2^{k_3-k_1-n_3+1}, 3^{n_3}\}$ results in a losing coalition $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. As the conditions (6) imply $k_1 \leq n_1$, the first coalition exists. The second coalition exists since $k_3 - k_1 - n_3 < n_2$ is equivalent to $k_3 - k_1 < n_2 + n_3$. This implies $1 \succ 2$.

Now, since $n_1 + n_2 \geq k_2$ and $k_2 < k_3$, there exists a minimal winning coalition $\{1^{\ell_1}, 2^{\ell_2}\}$ with $\ell_1 + \ell_2 = k_2$ and $\ell_2 \geq 1$. A replacement of 2 here with a 3 leads to a losing coalition, hence $2 \succ 3$. \square

12.2 Proofs of two Lemmata

Proof of Lemma 1. Suppose first that C is weighted but H is not. Then we have a certificate of nonweightedness $(U_1, \dots, U_j; V_1, \dots, V_j)$ for the game H . Let also X be any minimal winning coalition of G containing g (since g is not a dummy, it exists). Let $X' = X \setminus \{g\}$. Then

$$(X' \cup U_1, \dots, X' \cup U_j; X' \cup V_1, \dots, X' \cup V_j)$$

is a certificate of nonweightedness for C . Suppose now that C is weighted but G is not. Then let $(X_1, \dots, X_j; Y_1, \dots, Y_j)$ be a certificate of nonweightedness for G and W be a fixed minimal winning coalition W for H . Define

$$X'_i = \begin{cases} X_i \setminus \{g\} \cup W & \text{if } g \in X_i \\ X_i & \text{if } g \notin X_i \end{cases}$$

and

$$Y'_i = \begin{cases} Y_i \setminus \{g\} \cup W & \text{if } g \in Y_i \\ Y_i & \text{if } g \notin Y_i \end{cases}$$

Then, since $|\{i \mid g \in X_i\}| = |\{i \mid g \in Y_i\}|$, the following

$$(X'_1, \dots, X'_j; Y'_1, \dots, Y'_j)$$

is a trading transform in C . Moreover, it is a certificate of nonweightedness for C since all X'_1, \dots, X'_j are winning in C and all Y'_1, \dots, Y'_j are losing in C . So both assumptions are impossible. \square

Proof of Lemma 2. As g is more desirable than g' , there exists a coalition $X \subseteq P_G$, containing neither g nor g' such that $X \cup \{g\} \in W_G$ and $X \cup \{g'\} \notin W_G$. We may take X to be minimal with this property, then $X \cup \{g\}$ is a minimal winning coalition of G . Since g' is not dummy, there exist a minimal winning coalition Y containing g' . The coalition Y may contain g or may not. Firstly, assume that it does contain g . Since H is not an oligarchy there exist two distinct minimal winning coalitions of H , say Z_1 and Z_2 . Then we can find $z \in Z_1 \setminus Z_2$. Then the coalitions $U_1 = X \cup Z_1$ and $U_2 = (Y \setminus \{g\}) \cup Z_2$ are winning in $G \circ_g H$ and coalitions $V_1 = (X \cup \{g'\}) \cup (Z_1 \setminus \{z\})$ and $V_2 = Y \setminus \{g, g'\} \cup (Z_2 \cup \{z\})$ are losing in this game since $Z_1 \setminus \{z\}$ is losing in H and $Y \setminus \{g'\} = Y \setminus \{g, g'\} \cup \{g\}$ is losing in G . Since V_1 and V_2 are obtained when U_1 and U_2 swap players z and g' , the sequence of sets $(U_1, U_2; V_1, V_2)$ is a certificate of incompleteness for $G \circ_g H$.

Suppose now Y does not contain g . Let Z be any minimal winning coalition of H that has more than one player (it exists since H is not an anti-oligarchy). Let $z \in Z$. Then

$$(X \cup Z, Y; X \cup \{g'\} \cup (Z \setminus \{z\}), Y \setminus \{g'\} \cup \{z\})$$

is a certificate of incompleteness for $G \circ_g H$. \square

12.3 Nonweighted compositions of the irreducible ideal weighted games

Here we will consider two cases:

1. G_2 has at least one minimal winning coalition with cardinality at least 2.
2. $G_2 = A_n$, where $n \geq 2$.

We will start with the following general statement which will help us to resolve the first case.

Definition 6. Let $G = (P, W)$ be a simple game and $g \in P$. We say that a coalition X is g -winning if $g \notin X$ and $X \cup \{g\} \in W$.

Every winning coalition is of course g -winning but not the other way around.

Lemma 3. Let G be a game for which there exist coalitions X_1, X_2, Y_1, Y_2 such that both X_1 and X_2 do not contain g ,

$$(X_1, X_2; Y_1, Y_2) \tag{9}$$

is a trading transform, X_1 is winning, X_2 is g -winning and Y_1 and Y_2 are losing in G . Let also H be a game with a minimal winning coalition U which has at least two elements, then $C = G \circ_g H$ is not weighted.

Proof. If X_2 is winning in G , then there is nothing to prove since (9) is a certificate of nonweightedness for C , suppose not. Let $U = U_1 \cup U_2$, where U_1 and U_2 are losing in H . Then it is easy to check that

$$(X_1, X_2 \cup U; Y_1 \cup U_1, Y_2 \cup U_2)$$

is a certificate of nonweightedness for C . Indeed, X_1 and $X_2 \cup U$ are both winning in C and $Y_1 \cup U_1$ and $Y_2 \cup U_2$ are both losing. \square

The only exception in this case is when H consists of passers and dummies. We will have to consider this case separately.

Lemma 4. If G is of type \mathbf{B}_1 , \mathbf{B}_2 or \mathbf{B}_3 , g is any element of level 2, and H has a minimal winning coalition X which has at least two elements, then $G \circ_g H$ is not weighted.

Proof. Suppose G is of type \mathbf{B}_1 . Then let us consider the following trading transform

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1}, 2^{k_2-k_1-1}\}; \{1^{k_1-1}, 2^{k_2-k_1+1}\}, \{1^{k_1+1}, 2^{k_2-k_1-2}\})$$

(note that $k_2 - k_1 + 1 = n_2$ and $k_1 + 1 \leq n_1$ so there is enough capacity in both equivalence classes to make all coalitions involved legitimate). It is easy to check that the first coalition in this sequence is winning, the second is g -winning and the remaining two are losing. By Lemma 3 the result holds.

Suppose now G is of type \mathbf{B}_2 , then $k_2 = k_1 + 1 \leq n_2$. Let $k_1 = k$. Then we can apply Lemma 3 to the trading transform

$$(\{1^k\}, \{2^k\}; \{1^{\lfloor \frac{k}{2} \rfloor}, 2^{\lceil \frac{k}{2} \rceil}\}, \{1^{\lceil \frac{k}{2} \rceil}, 2^{\lfloor \frac{k}{2} \rfloor}\}),$$

where $\{1^k\}$ is winning, $\{2^k\}$ is g -winning and the remaining two coalitions are losing.

If G is of type \mathbf{B}_3 , then $n_2 < k_2 = k_1 + 1$. We again let $k = k_1$. In this case we can apply Lemma 3 to the trading transform

$$(\{1^k\}, \{1^{k-2}, 2^2\}; \{1^{k-1}, 2\}, \{1^{k-1}, 2\}),$$

where the first coalition is winning, the second is g -winning (we use $n_2 \geq 3$ here) and the two remaining coalitions are losing. \square

Lemma 5. *If G is of type \mathbf{T}_1 or \mathbf{T}_3 , g is any element of level 3, and H has a minimal winning coalition X which has at least two elements, then $C = G \circ_g H$ is not weighted.*

Proof. If G is of type \mathbf{T}_1 . Then let us consider the following trading transform

$$(\{1^{k_1}\}, \{2^{k_2}, 3^{k_3-k_2-1}\}; \{1^{k_1-1}, 2\}, \{1, 2^{k_2-1}, 3^{k_3-k_2-1}\}).$$

Lemma 3 is applicable to it so C is not weighted.

Suppose G is of type \mathbf{T}_3 . Then let us consider the following trading transform

$$(\{1^{k_2-n_2}, 2^{n_2}\}, \{1^{k_1}, 2^{n_2-1}, 3^{n_3-1}\}; \{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_1}, 2^{n_2}, 3^{n_3-2}\}).$$

Since $n_3 > 1$ all coalitions exist. Lemma 3 is now applicable and shows that C is not weighted. This proves the lemma. \square

We will now deal with the second case. Denote players of A_n by P_{A_n} .

Proposition 13. *Let G_1 be an ideal weighted indecomposable simple game of types \mathbf{B}_1 , \mathbf{B}_3 , \mathbf{T}_1 , and \mathbf{T}_3 , and g be a player from the least desirable level of G_1 , then $G = G_1 \circ_g A_n$ is not weighted.*

Proof. Let G_1 be of type \mathbf{B}_1 . The only shift-minimal winning coalition of G_1 is of the form $\{1^{k_1}, 2^{k_2-k_1}\}$, where $n_1 > k_1 > 0$, $k_2 - k_1 = n_2 - 1 > 1$. Composing over a player of level 2 of G_1 gives shift-minimal winning coalitions of types $\{1^{k_1}, 2^{k_2-k_1}\}$ and $\{1^{k_1}, 2^{k_2-k_1-1}, 3\}$. Thus the game is not weighted due to the following certificate of nonweightedness:

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1}, 2^{k_2-k_1-1}, 3\}; \{1^{k_1-1}, 2^{k_2-k_1+1}, 3\}, \{1^{k_1+1}, 2^{k_2-k_1-2}\}).$$

Since in a game of type \mathbf{B}_1 we have $k_2 - k_1 + 1 = n_2$ and $k_1 + 1 \leq n_1$, then all the coalitions in this trading transform exist.

Now consider \mathbf{B}_3 . Its shift-minimal winning coalition have types $\{1^{k_1}\}, \{1^{k_2-n_2}, 2^{n_2}\}$. Composing over a player of level 2 of G_1 gives the following types of winning coalitions $\{1^{k_1}\}, \{1^{k_2-n_2}, 2^{n_2-1}, 3\}$ in G . The game is not weighted due to the following certificate of nonweightedness:

$$(\{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_2-n_2}, 2^{n_2-1}, 3\}; \{1^{k_2-n_2+1}, 2^{n_2-2}\}, \{1^{k_2-n_2-1}, 2^{n_2}, 3^2\}).$$

Note that $k_2 - n_1 + 1 < k_1 \leq n_1$ and $n_2 > 2$ in \mathbf{B}_3 , so all the coalitions in this transform exist.

Now consider \mathbf{T}_1 . Since its levels 2 and 3 form a subgame of type \mathbf{B}_1 , composing it with A_n over a player of level 3, as was proved, will result in a nonweighted game.

Let us consider \mathbf{T}_3 , where the shift-minimal winning coalition are $\{1^{k_2-n_2}, 2^{n_2}\}, \{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. If we compose over a player of level 3 of G_1 , then the resulting game will have shift-minimal coalitions of the following type $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}$, where now elements of $G_2 = A_n$ will form level 4. Then we can show that the composition $G_1 \circ G_2$ is not weighted due to the following certificate of nonweightedness:

$$(\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}, \{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}, 4\}; \{1^{k_1+1}, 2^{k_3-k_1-n_3}, 3^{n_3-2}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}, 4^2\}).$$

The coalition $\{1^{k_1+1}, 2^{k_3-k_1-n_3}, 3^{n_3-2}\}$ is losing because in \mathbf{T}_3 we have $k_3 - k_1 - n_3 = n_2 - 1$ and also $k_2 - n_2 > k_1$, meaning $(k_1 + 1) + (k_3 - k_1 - n_3) = k_1 + 1 + n_2 - 1 \leq k_2 - n_2 + n_2 - 1 = k_2 - 1$ Also in total it contains less than k_3 elements. The coalition $\{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}, 4^2\}$ is easily seen to be losing as well.

Now all that remains for the proof of Theorem 9 is to consider the cases when g is not from the least desirable level of G_1 which may happen only when it is of types \mathbf{T}_1 and \mathbf{T}_3 . These cases are similar to those that have been already considered and we delegate them to the Appendix. \square

12.4 End of proof of Theorem 9

Here we have to deal with the hypothetical possibility that G does not fall into categories (i) and (ii). Then we know that G_1 has at least two desirability levels and g is not from the least desirable level. Also Lemma 2 implies that in this case $G_2 = A_n$ or $G_2 = U_n$ for some $n \geq 2$. Let us deal with $G_2 = A_n$ first. We need the following

Lemma 6. *Let $G = (P, W)$ be a game where player g is strictly more desirable than player g' . Suppose also that we can find two coalitions X_1 and X_2 in G such that*

$$g' \notin X_1, \quad X_1 \cup \{g\} \in W, \quad X_1 \cup \{g'\} \in L; \quad (10)$$

$$g' \in X_2, \quad X_2 \cup \{g\} \in W, \quad X_2 \setminus \{g'\} \cup \{g\} \in L. \quad (11)$$

Then the composition $C = G \circ_g A_n$, $n \geq 2$, is not complete.

Proof. Let $a, b \in A_n$. We have the following certificate of incompleteness:

$$(X_1 \cup \{a\}, X_2 \cup \{b\}; X_1 \cup \{g'\}, X_2 \setminus \{g'\} \cup \{a, b\}).$$

Indeed, both X_1 and X_2 win with g in G and both $\{a\}$ and $\{b\}$ are winning coalitions in H , so $X_1 \cup \{a\}$ and $X_2 \cup \{b\}$ are winning in C . On the other hand $X_1 \cup \{g'\}$ and $X_2 \cup \{g'\}$ are losing in G and the latter even losing with g so $X_1 \cup \{g'\}$ and $X_2 \setminus \{g'\} \cup \{a, b\}$ are both losing in C . This proves the lemma. \square

Lemma 7. *Let G be an indecomposable simple game of one of the types $\mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{T}_1$, and \mathbf{T}_3 , and let g be a player of G which is not from the least desirable level. Then the composition $G \circ_g A_n$ is not complete for all $n \geq 2$.*

Proof. Let us first consider the case where g is from the most desirable level of G . We will apply Lemma 6 to show that $G \circ_g A_n$ is not complete. So in what follows we show that for each case there exists $g, g' \in P$ and coalitions X_1 and X_2 of G which satisfy the conditions of Lemma 6. In the following three cases, g is a player of level 1 and g' is a player of level 2.

- (i) \mathbf{B}_1 : X_1 is of type $\{1^{k_1-1}, 2^{k_2-k_1}\}$, and X_2 is of type $\{1^{k_1-1}, 2^{k_2-k_1}\}$;
- (ii) \mathbf{B}_2 : X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{2^{k_1}\}$;
- (iii) \mathbf{B}_3 : X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{1^{k_2-n_2}, 2^{n_2-1}\}$.

And for the following three cases, g is a player of level 1 and g' is a player of level 3.

- (iv) \mathbf{T}_1 : X_1 is of type $\{1^{k_1-1}\}$, and X_2 is of type $\{2^{k_2}, 3^{k_3-k_2-1}\}$;
- (v) \mathbf{T}_3 : X_1 is of type $\{1^{k_2-n_2-1}, 2^{n_2}\}$, and X_2 is of type $\{1^{k_1-1}, 3^{k_3-k_1}\}$.

All is left is to consider composing games of the \mathbf{T} types over a player of level 2. We start with \mathbf{T}_1 . As we know any game of type \mathbf{T}_1 contains a subgame of type \mathbf{B}_1 when we restrict it to levels 2 and 3 only. For that subgame 2 is the most desirable player so noncompleteness follows from (i).

Finally we look at \mathbf{T}_3 and suppose now g is a player of level 2 and g' is a player of level 3. Here X_1 can be taken of type $\{1^{k_2-n_2}, 2^{n_2-1}\}$. Indeed, if we add g to X_1 it becomes winning but it loses with g' . Then X_2 can be taken of type $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3-1}\}$. We can add g to X_2 since $n_2 \geq k_3 - k_1 - n_3 + 1$ and it becomes winning. We can add g and remove g' from it since $n_3 \geq 2$. X_2 will remain losing after that. So we can again apply Lemma 6 to conclude that the composition is not complete. This completes the study of compositions where G_2 is the anti-unanimity game A_n , such that the compositions are not over the least desirable level of G_1 . \square

Finally, we consider compositions where G_2 is the unanimity game U_n . It turns out that none of these compositions give a weighted game either, which is what we show next.

Lemma 8. *Let $G_1 = (P, W)$ be a simple game of one of the types \mathbf{B}_1 , \mathbf{B}_2 , \mathbf{B}_3 , \mathbf{T}_1 , and \mathbf{T}_3 and let $g \in P$ be a player not from the least desirable level of G_1 . Then the composition $G = G_1 \circ_g U_n$ is not weighted.*

Proof. Let U_n be defined on P_{U_n} , and let $Z = P_{U_n}$. We start with G_1 being of type \mathbf{B}_1 . A shift-minimal winning coalition of G_1 has the only form $\{1^{k_1}, 2^{k_2-k_1}\}$, where $k_1 < n_1$. We compose over level 1 of G_1 . Then G is nonweighted by Lemma 3 applied to the following trading transform

$$(\{1^{k_1}, 2^{k_2-k_1}\}, \{1^{k_1-1}, 2^{k_2-k_1}\}; \{1^{k_1}, 2^{k_2-k_1-1}\}, \{1^{k_1-1}, 2^{k_2-k_1+1}\}).$$

This is because the first coalition is winning, the second coalition is 1-winning and the remaining two are losing. Note that $k_2 - k_1 + 1 = n_2 \geq 2$ in a game of type \mathbf{B}_1 , so the coalition $\{1^{k_1-1}, 2^{k_2-k_1+1}\}$ is allowed.

Now let G_1 be of type \mathbf{B}_2 . The shift-minimal winning coalitions of G_1 here are $\{1^{k_1}\}, \{2^{k_1+1}\}$, and if we compose with U_n over level 1 of G_1 , then G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{2^{k_1+1}\}, \{1^{k_1-1}\}; \{1^{k_1-1}, 2\}, \{2^{k_1}\}).$$

This is because the first coalition is winning and the second is 1-winning. The remaining two are losing.

Now let G_1 be of type \mathbf{B}_3 . Recall that in a game of type \mathbf{B}_3 we have $k_1 \leq n_1$, and also $k_2 - n_2 < k_1$. So the shift-minimal winning coalitions of G_1 are $\{1^{k_1}\}, \{1^{k_2-n_2}, 2^{n_2}\}$. If we compose with U_n over level 1 of G_1 , then G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{1^{k_2-n_2}, 2^{n_2}\}, \{1^{k_1-1}\}; \{1^{k_2-n_2}, 2^{n_2-1}\}, \{1^{k_1-1}, 2\}).$$

This is because the second coalition is 1-winning.

Next we look at the games \mathbf{T}_1 , and \mathbf{T}_3 . Since they have three levels each, then we need to consider what happens when composing over level 1 and when composing over level 2 separately. Let us start with \mathbf{T}_1 .

The shift-minimal winning coalitions of G_1 are $\{1^{k_1}\}$ and $\{2^{k_2}, 3^{k_3-k_2}\}$. Here we need to consider two compositions, one over level 1, and one over level 2.

Case (i). If we compose with U_n over level 1 of G_1 then G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{1^{k_1-1}\}, \{2^{k_2}, 3^{k_3-k_2}\}; \{1^{k_1-1}, 2\}, \{2^{k_2-1}, 3^{k_3-k_2}\}).$$

This is because the first coalition is 1-winning, the second is winning and the remaining two are losing.

Case (ii). If we compose with U_n over level 2 of G_1 , then G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{1^{k_1}\}, \{2^{k_2-1}, 3^{k_3-k_2}\}; \{1^{k_1-1}, 2\}, \{1, 2^{k_2-2}, 3^{k_3-k_2}\}).$$

This is because the first coalition is winning, the second coalition is 2-winning and the remaining two are losing.

Finally, let G_1 be of type \mathbf{T}_3 . The shift-minimal winning coalitions of G_1 are $\{1^{k_2-n_2}, 2^{n_2}\}$ and $\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}$. Here we again need to consider two compositions, one over level 1, one over level 2.

Case (i). If we compose G_1 with U_n over level 1 of G_1 , then since $k_1 \leq n_1$, the game G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{1^{k_1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3}, 3^{n_3}\}; \{1^{k_1}, 2^{k_3-k_1-n_3-1}, 3^{n_3}\}, \{1^{k_1-1}, 2^{k_3-k_1-n_3+1}, 3^{n_3}\}).$$

This is because the first coalition is winning, the second coalition is 1-winning and the two remaining ones are losing. Note that $k_3 - k_1 - n_3 + 1 \leq n_2$ in a game of type \mathbf{T}_3 (see Theorem 7), so the last coalition exists.

Case (ii). If we compose with U_n over level 2 of G_1 , then G is nonweighted by Lemma 3 applied to the following trading transform:

$$(\{1^{k_2-n_2}, 2^{n_2-1}\}, \{1^{k_1}, 3^{k_3-k_1}\}; \{1^{k_2-n_2}, 2^{n_2-1}, 3\}, \{1^{k_1}, 3^{k_3-k_1-1}\}).$$

Indeed, by (6) $k_2 - n_2 \leq n_1$ and $k_2 < k_3$. Thus the first coalition exists and is 2-winning, the second is winning and the remaining two are losing. \square

We see that none of the six games above produce a weighted game when composed with U_n over a player not from the least desirable level of the first game.